PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Commissioner
US Department of Commerce
United States Patent and Trademark
Office, PCT
2011 South Clark Place Room
CP2/5C24
Arlington, VA 22202
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing: 01 February 2001 (01.02.01)	
International application No.: PCT/CH99/00336	Applicant's or agent's file reference: 150973.1/DV/tr
International filing date: 21 July 1999 (21.07.99)	Priority date:
Applicant: HUBER, Adriano	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International preliminary Examining Authority on:

29 April 2000 (29.04.00)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO **34, chemin des Colombettes** **1211 Geneva 20, Switzerland**	Authorized officer: J. Zahra
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

Form PCT/IB/331 (July 1992)

3794429

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

To:

BOVARD AG
Optingenstrasse 16
CH-3000 Bern 25
SUISSE

NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92bis.1 and Administrative Instructions, Section 422)

Date of mailing (day/month/year)
18 April 2001 (18.04.01)

Applicant's or agent's file reference
150973.1/DV/tr

IMPORTANT NOTIFICATION

International application No.
PCT/CH99/00336

International filing date (day/month/year)
21 July 1999 (21.07.99)

1. The following indications appeared on record concerning:

[X] the applicant [ ] the inventor [ ] the agent [ ] the common representative

Name and Address
SWISSCOM AG
Alte Tiefenaustrasse 6
CH-3050 Bern
Switzerland

State of Nationality: CH
State of Residence: CH
Telephone No.:
Facsimile No.:
Teleprinter No.:

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

[ ] the person [X] the name [X] the address [ ] the nationality [ ] the residence

Name and Address
SWISSCOM MOBILE AG
Schwarztorstrasse 61
CH-3050 Bern
Switzerland

State of Nationality: CH
State of Residence: CH
Telephone No.:
Facsimile No.:
Teleprinter No.:

3. Further observations, if necessary:

4. A copy of this notification has been sent to:

[X] the receiving Office
[ ] the International Searching Authority
[ ] the International Preliminary Examining Authority
[ ] the designated Offices concerned
[X] the elected Offices concerned
[ ] other:

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer
G. Bähr

Telephone No.: (41-22) 338.83.38

003968344

Form PCT/IB/306 (March 1994)

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
1. Februar 2001 (01.02.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/08435 A1

(51) Internationale Patentklassifikation[7]: H04Q 7/38

(21) Internationales Aktenzeichen: PCT/CH99/00336

(22) Internationales Anmeldedatum:
21. Juli 1999 (21.07.1999)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: SWISSCOM AG [CH/CH]; Alte Tiefenaustrasse 6, CH-3050 Bern (CH).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: HUBER, Adriano [CH/CH]; Via F. Caponelli, 35, CH-6600 Locarno (CH).

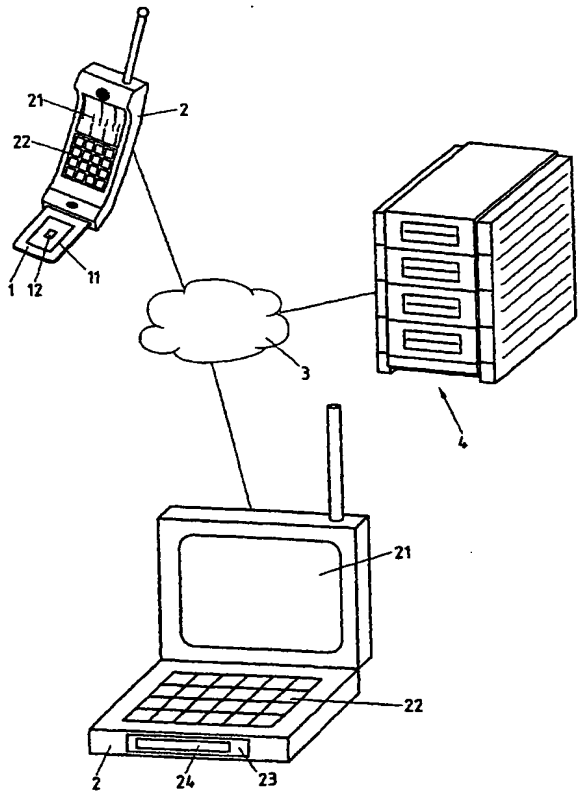
(74) Anwalt: BOVARD AG; Optingenstrasse 16, CH-3000 Bern 25 (CH).

(81) Bestimmungsstaaten *(national)*: AE, AL, AM, AT, AT (Gebrauchsmuster), AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Gebrauchsmuster), DE, DE (Gebrauchsmuster), DK, DK (Gebrauchsmuster), EE, EE (Gebrauchsmuster), ES, FI, FI (Gebrauchsmuster), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK,

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD AND ASSOCIATED DEVICES FOR SETTING THE SECURITY LEVEL OF CRYPTOGRAPHIC FUNCTIONS

(54) Bezeichnung: VERFAHREN UND GEEIGNETE VORRICHTUNGEN, UM DEN SICHERHEITSGRAD VON KRYPTOGRAPHIEFUNKTIONEN ZU SETZEN



(57) Abstract: The invention relates to a method and associated devices for setting the security level of cryptographic functions (11, 23) used in communication terminals (2) according to situation. In a telecommunication terminal (2), especially in a mobile telephone (2), situation parameters, such as an identification code of a country where the telecommunication terminal (2) is temporarily present, are received in a secured manner from a secure source (3, 4) via a telecommunication network (3), especially a mobile telephone network (3). In addition, in said telecommunication network (2), security parameters, such as the maximum acceptable length (in bits) of cryptographic keys, are determined on the basis of the received situation parameters, and said security parameters are used by the cryptographic functions (11, 23) and determine the security level.

(57) Zusammenfassung: Verfahren und geeignete Vorrichtungen, um den Sicherheitsgrad von in Kommunikationsendgeräten (2) verwendeten Kryptographiefunktionen (11, 23) situationsabhängig zu setzen, wobei in einem Kommunikationsendgerät (2), insbesondere einem Mobilfunkgerät (2), situationsanzeigende Parameter, beispielsweise ein Ländercode des Landes, in welchem sich das Kommunikationsendgerät (2) momentan befindet, von einer sicheren Quelle (3, 4) gesichert über ein Telekommunikationsnetz (3), insbesondere ein Mobilfunknetz (3), entgegengenommen werden, und wobei im Kommunikationsendgerät (2) basierend auf entgegengenommenen situationsanzeigenden Parametern Sicherheitsparameter, beispielsweise die maximal zulässige (Bit-) Länge von kryptographischen Schlüsseln, bestimmt werden, welche Sicherheitsparameter von den Kryptographiefunktionen (11, 23) verwendet werden und den Sicherheitsgrad bestimmen.

WO 01/08435 A1

SK (Gebrauchsmuster), SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) **Bestimmungsstaaten** *(regional)*: ARIPO-Patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:
— *Mit internationalem Recherchenbericht.*

Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Verfahren und geeignete Vorrichtungen, um den Sicherheitsgrad von Kryptographiefunktionen zu setzen

Die vorliegende Erfindung betrifft ein Verfahren und geeignete Vorrichtungen, um den Sicherheitsgrad von Kryptographiefunktionen zu setzen. Insbesondere betrifft die vorliegende Erfindung ein Verfahren und geeignete Vorrichtungen, um den Sicherheitsgrad von in Kommunikationsendgeräten verwendeten Kryptographiefunktionen zu setzen.

Um vertrauliche Daten bei der Übertragung über Telekommunikationsnetze, insbesondere bei der Übertragung über Mobilfunknetze, vor dem Zugriff durch unberechtigte Drittparteien zu schützen ist es heutzutage allgemein üblich, Kryptographieverfahren einzusetzen, mittels welchen die vertraulichen Daten vor der Übertragung über das Telekommunikationsnetz beim Sender verschlüsselt und nach der Übertragung über das Telekommunikationsnetz beim Empfänger entschlüsselt werden. Verschiedene Kryptographieverfahren weisen unterschiedliche Sicherheitsgrade auf, die von Sicherheitsparametern, wie den verwendeten Kryptographiealgorithmen und den darin verwendeten kryptographischen Schlüsseln, insbesondere der Bitlänge der darin verwendeten Schlüssel, abhängen. Die Anwender der Kryptographieverfahren, beispielsweise Dienstleister wie Finanzinstitute oder Dienstleistungsnehmer wie Bankkunden, wünschen im Allgemeinen einen hohen Sicherheitsgrad. Allerdings gebieten nationale Interessen von gewissen Ländern, in denen beispielsweise betreffende kryptographische Produkte hergestellt werden und/oder in denen Eigentümer von entsprechenden Schutzrechten beheimatet sind, die Verbreitung von Kryptographieprodukten, beispielsweise ab gewissen vordefinierten Sicherheitsgraden oder unter Verwendung von gewissen vordefinierten Sicherheitsparametern, über die Landesgrenzen hinweg oder zumindest in gewisse definierte Länder zu unterbinden. Für die Hersteller von solchen Kryptographieprodukten, die in ihrem eigenen wirtschaftlichen Interesse ihre Produkte möglichst weltweit vermarkten möchten, die aber den nationalen Vorschriften und gesetzlichen Bestimmungen unterliegen, stellt sich nun das Problem, wie sie ihre eigenen Interessen unter Einhaltung der nationalen Bestimmungen möglichst effizient verfolgen können. Die Herstellung, Verwaltung und Wartung von verschiedenen Kryptographieprodukten für verschiedene

Märkte erweist sich dabei als keine optimale Lösung, da die Produkteversionen und insbesondere auch Kombinationen mit anderen Produkten, in welche die Kryptographieprodukte integriert werden, viel zu zahlreich sind und einen unwirtschaftlichen Mehraufwand mit sich bringen. In alternativen Lösungen wird zwar das gleiche Produkt überallhin ausgeliefert, aber gewisse Teile, die den national auferlegten Restriktionsbestimmungen unterliegen, werden vor der Produktauslieferung durch Schalter deaktiviert, beispielsweise mittels softwaremässigen Schaltern, die durch Setzen von sogenannten Flags ein- respektive ausgeschaltet werden. Das Problem dieser alternativen Lösung besteht darin, dass diese Schalter oft auch durch Drittparteien verändert werden können, beispielsweise durch sogenannte Programmpatches, die die erwähnten Flags manipulieren können.

Es ist eine Aufgabe dieser Erfindung, ein neues und besseres Verfahren sowie dafür geeignete Vorrichtungen vorzuschlagen, welche es ermöglichen, den Sicherheitsgrad von in Kommunikationsendgeräten verwendeten Kryptographiefunktionen, insbesondere situationsabhängig, zu setzen.

Gemäss der vorliegenden Erfindung wird dieses Ziel insbesondere durch die Elemente der unabhängigen Ansprüche erreicht. Weitere vorteilhafte Ausführungsformen gehen ausserdem aus den abhängigen Ansprüchen und der Beschreibung hervor.

Dieses Ziel wird durch die vorliegende Erfindung insbesondere dadurch erreicht, dass in einem Kommunikationsendgerät, welches über Telekommunikationsnetze kommuniziert, situationsanzeigende Parameter von einer sicheren Quelle, die beispielsweise mittels einem digitalen Zertifikat als sichere Quelle authentifiziert wird, gesichert über das Telekommunikationsnetz entgegengenommen werden, beispielsweise direkt, ohne Beeinflussungsmöglichkeiten durch andere Elemente, aus einem chiffrierten Datenobjekt mit zertifiziertem Schlüssel oder als nicht beeinflussbarer Bestandteil des im betreffenden Telekommunikationsnetz verwendeten Protokolls, und dass im Kommunikationsendgerät basierend auf entgegengenommenen situationsanzeigenden Parametern Sicherheitsparameter, zum Beispiel die maximal zulässige Länge von kryptographischen Schlüsseln oder zugelassene

kryptographische Algorithmen, bestimmt werden, welche Sicherheitsparameter von Kryptographiefunktionen verwendet werden und den Sicherheitsgrad bestimmen. Der Vorteil dieses Verfahrens besteht darin, dass der Sicherheitsgrad von im Kommunikationsendgerät verwendeten Kryptographiefunktionen, respektive von diesen Kryptographiefunktionen verwendete Sicherheitsparameter, situationsabhängig und dynamisch gesetzt werden kann/können, so dass keine unterschiedlichen Kryptographieprodukte in verschiedene Zielmärkte geliefert werden müssen und vom Hersteller keine Schalter statisch gesetzt werden müssen, deren Wirkung durch ein einmaliges Überschreiben rückgängig gemacht werden kann.

In einer Ausführungsvariante enthalten mindestens gewisse situationsanzeigende Parameter dienstspezifische Angaben, beispielsweise Angaben betreffend den Typ des betreffenden Dienstes, die von einem Dienstserver, beispielsweise ein E-Mail-Server oder ein File-Transfer-Server, von welchem das genannte Kommunikationsendgerät Dienste bezieht, gesichert, beispielsweise verschlüsselt und/oder als Bestandteil eines digitalen, chiffrierten Datenobjekts mit zertifiziertem Schlüssel, über das Telekommunikationsnetz an das Kommunikationsendgerät übertragen werden. Der Vorteil, dienstspezifische Angaben bei der Festlegung des Sicherheitsgrades von Kryptographiefunktionen zu berücksichtigen besteht darin, dass verschiedene Sicherheitsgrade für unterschiedliche Dienste, beispielsweise höhere Sicherheitsgrade für Finanzdienste als für E-Mail-Dienste, für verschiedene Ebenen von Diensten, beispielsweise unterschiedliche Sicherheitsgrade auf der Transportebene und auf der Applikationsebene, und für verschiedene Anwendungen von Diensten, beispielsweise unterschiedliche Sicherheitsgrade für File-Transfer in einer Finanzanwendung (Finanzdienst) als in einer Datenbankanwendung (Datendienst) vorgeschrieben und gesetzt werden können.

In einer Ausführungsvariante enthalten mindestens gewisse situationsanzeigende Parameter Angaben über den zulässigen Sicherheitsgrad, beispielsweise gemäss einer international vereinbarten Norm oder zulässige Sicherheitsparameter, beispielsweise Angaben über spezifische zugelassene kryptographische Algorithmen, die von einem Dienstserver, von welchem das

Kommunikationsendgerät Dienste bezieht, gesichert, beispielsweise verschlüsselt und/oder als Bestandteil eines digitalen, chiffrierten Datenobjekts mit zertifiziertem Schlüssel, über das Telekommunikationsnetz an das Kommunikationsendgerät übertragen werden.

In einer Ausführungsvariante sind mindestens gewisse der Kommunikationsendgeräte Mobilfunkgeräte, beispielsweise Mobilfunktelefone oder kommunikationsfähige Lap- oder Palmtop-Computer für GSM- (Global System for Mobile Communication), UMTS- (Universal Mobile Telephone System), oder andere, beispielsweise satellitenbasierte, Mobilfunknetze und mindestens gewisse situationsanzeigende Parameter enthalten einen Ländercode, der von einem Mobilfunknetz, in welchem das Mobilfunkgerät roamt, an das Mobilfunkgerät übertragen wird. Die Anwendung des erfindungsgemässen Verfahrens in Mobilgeräten, insbesondere unter Verwendung von Ländercodes als situationsanzeigende Parameter, hat den Vorteil, dass der Sicherheitsgrad der verwendeten Kryptographiefunktionen dynamisch an die in einem betreffenden Aufenthaltsland geltenden Restriktionen betreffend zulässiger maximalen Sicherheitsgrade angepasst werden können.

An dieser Stelle soll erwähnt werden, dass sich die vorliegende Erfindung neben dem erfindungsgemässen Verfahren auch auf ein erfindungsgemässes Kommunikationsendgerät, insbesondere auf ein mobiles Kommunikationsendgerät, beispielsweise ein Mobilfunktelefon oder ein kommunikationsfähiger Lap- oder Palmtop-Computer für GSM-, UMTS- oder andere, beispielsweise satellitenbasierte, Mobilfunknetze, auf eine erfindungsgemässe Chipkarte, beispielsweise eine SIM-Karte (Subscriber Identification Module), die in einem Kommunikationsendgerät eingesetzt werden kann, sowie auf einen erfindungsgemässen Computer-lesbaren Datenträger und auf ein erfindungsgemässes Computerprogrammelement bezieht.

Nachfolgend wird eine Ausführung der vorliegenden Erfindung anhand eines Beispieles beschrieben. Das Beispiel der Ausführung wird durch folgende einzige beigelegte Figur illustriert:

Figur 1 zeigt ein Blockdiagramm mit einer schematischen Darstellung eines ersten Mobilfunkgeräts mit einer Chipkarte, eines zweiten Mobilfunkgeräts sowie eines Dienstservers, die mit einem Mobilfunknetz verbunden sind.

In der Figur 1 bezieht sich die Bezugsziffer 3 auf ein Telekommunikationsnetz, insbesondere ein Mobilfunknetz 3, beispielsweise ein GSM-, UMTS, oder ein anderes, zum Beispiel ein satellitenbasiertes, Mobilfunknetz 3, über welches Kommunikationsendgeräte 2, insbesondere Mobilfunkgeräte 2, miteinander oder mit Dienstservern 4, beispielsweise ein File-Transfer-Server, ein Finanzserver, ein Datenbankserver, oder ein E-Mail-Server, kommunizieren, das heisst insbesondere auch Daten austauschen, können.

Die Mobilfunkgeräte 2 umfassen ein erfindungsgemässes Sicherheitsgradbestimmungsmodul 12, 24, welches vorzugsweise ein programmiertes Softwaremodul ist, das sich in einem geeigneten, von Benutzern nicht manipulierbaren Speicher im Mobilfunkgerät 2 oder auf einer mit dem Mobilfunkgerät 2 verbundenen Chipkarte 1 befindet. Das Sicherheitsgradbestimmungsmodul 12, 24 ist beispielsweise Bestandteil von Kryptographiefunktionen 11, 23, die in den Mobilfunkgeräten 2 verwendet werden. Funktionen des Sicherheitsgradbestimmungsmoduls 12, 24 werden in einem Prozessor im Mobilfunkgerät 2 oder auf der mit dem Mobilfunkgerät 2 verbundenen Chipkarte 1 ausgeführt.

Die Hauptfunktion des Sicherheitsgradbestimmungsmoduls 12, 24 besteht darin, den Sicherheitsgrad der im Mobilfunkgerät 2 verwendeten Kryptographiefunktionen 11, 23, respektive von diesen Kryptographiefunktionen 11, 23 verwendete Sicherheitsparameter situationsabhängig zu setzen. Die aktuelle Situation wird dabei von sogenannten situationsanzeigenden Parametern bestimmt, welche vom Sicherheitsgradbestimmungsmodul 12, 24 von sicheren Quellen gesichert entgegengenommen werden.

Als situationsanzeigende Parameter gelten beispielsweise das betreffende Land, in welchem das Mobilfunkgerät 2 betrieben wird, oder dienstspezifische Angaben, beispielsweise der betreffende Dienst oder Diensttyp eines Dienstservers 4, welcher vom Mobilfunkgerät 2 benutzt wird, oder Anga-

ben betreffend Protokolle, respektive Protokollebenen, die von diesem Dienst verwendet werden oder andere Angaben über den betreffenden Dienst, respektive Angaben darüber, wie ein bestimmter Dienst, respektive eine verfügbare Funktion, angewendet wird, beispielsweise kann für die Verwendung von File-Transfer-Funktionen in einer Finanzanwendung (Finanzdienst) ein höherer Sicherheitsgrad zulässig sein als für deren Verwendung in einer Datenbankanwendung (Datendienst). Es ist auch möglich, dass die situationsanzeigenden Parameter direkte und spezifische Angaben betreffend den zu verwendenden Sicherheitsparametern oder des maximal zulässigen und/oder zu verwendenden Sicherheitsgrades enthalten, wobei Angaben betreffend den Sicherheitsgrad vorzugsweise auf einer internationalen Norm beruhen.

Als Sicherheitsparameter gelten beispielsweise die (Bit-) Länge von verwendeten kryptographischen Schlüsseln oder die Benennung von spezifischen zu verwendenden kryptographischen Algorithmen aus einer Reihe von möglichen alternativen Algorithmen.

Eine Quelle von situationsanzeigenden Parametern, beispielsweise der Dienstserver 4, kann beispielsweise dann als sicher akzeptiert werden, wenn von ihr ein digitales (signiertes) Zertifikat erhalten wird, welches die Quelle authentifiziert. Die Netzwerkinfrastruktur des Mobilfunknetzes 3 kann in dem Sinne als sichere Quelle betrachtet werden, als nicht beeinflussbare Bestandteile des im Mobilfunknetz 3 verwendeten Protokolls als situationsanzeigende Parameter verwendet werden.

Situationsanzeigende Parameter werden in dem Sinne gesichert über das Telekommunikationsnetz entgegengenommen, als sie direkt, ohne Beeinflussungsmöglichkeiten durch andere Elemente, beispielsweise aus einem digitalen, chiffrierten Datenobjekt mit zertifiziertem Schlüssel oder als nicht beeinflussbarer Bestandteil aus Protokolldateneinheiten des im betreffenden Mobilfunknetz 3 verwendeten Protokolls entnommen werden.

Zur Umsetzung von entgegengenommenen situationsanzeigenden Parametern in zu verwendende Sicherheitsparameter verfügt das Sicherheitsgradbestimmungsmodul 12, 24 beispielsweise über entsprechende, vom Be-

nutzer nicht manipulierbare Tabellen oder entsprechende Programminstruktionen, mittels welchen den aktuellen entgegengenommenen situationsanzeigenden Parametern entsprechende Sicherheitsparameter zugeordnet werden. Da sich die zulässigen Sicherheitsgrade, respektive Sicherheitsparameter, insbesondere in verschiedenen Ländern im Laufe der Zeit ändern können, ist es möglich, diese Tabellen, respektive diese Programminstruktionen, unter Zuhilfenahme von sicheren kryptographischen Funktionen in einem zuständigen Dienstleistungszentrum oder über das Mobilfunknetz 3 zu aktualisieren.

Situationsanzeigende Parameter werden vom Sicherheitsgradbestimmungsmodul 12, 24 beispielsweise dadurch erfasst, dass über das Mobilfunknetz 3 empfangene Protokolldateneinheiten darauf überprüft werden, ob sie einen neuen Ländercode enthalten (MCC, Mobile Country Code), oder dass über das Mobilfunknetz 3 empfangene, chiffrierte Datenobjekte mit zertifiziertem Schlüssel (digitale Zertifikate) darauf geprüft werden, ob sie situationsanzeigende Parameter enthalten, zum Beispiel dienstspezifische Angaben wie beispielsweise eine Angabe betreffend den aktuellen Diensttyp, zum Beispiel E-Mail oder File-Transfer, oder betreffend die Anwendung eines Dienstes, beispielsweise die Verwendung von File-Transfer in einer Finanzanwendung (Finanzdienst) oder in einer Datenbankanwendung (Datendienst). Der Fachmann wird verstehen, dass es auch möglich ist, für die Bestimmung von situationsanzeigenden Parametern, respektive für die Bestimmung von Sicherheitsgraden und/oder den zu verwendenden Sicherheitsparametern spezielle Protokolle zu definieren, die zwischen Kommunikationsendgeräten 2, insbesondere den darin enthaltenen Sicherheitsgradbestimmungsmodul 12, 24 und Dienstservern 4 eingesetzt werden können.

Es soll hier auch erwähnt werden, dass situationsanzeigende Parameter und die Differenzierung der zu verwendenden Sicherheitsgrade, respektive Sicherheitsparameter, auch individuelle Protokollebenen betreffen können, beispielsweise Protokollebenen gemäss dem siebenschichtigen OSI-Referenzmodell (Open Systems Interconnection) der ISO (International Standards Organisation), so dass beispielsweise für die Applikationsebene (OSI-Schicht 7) und die Transportebene (OSI-Schicht 4) verschiedene Restriktionen betreffend zulässige Sicherheitsgrade anwendbar sind. Es sollte auch erwähnt wer-

den, dass typischerweise mehrere situationsanzeigende Parameter kombiniert werden, so dass beispielsweise im Land „X" und im Land „Y" die gleichen Restriktionen auf der Transportebene gelten können, aber für das Land „X" strengere Restriktionen auf der Applikationsebene gelten als für das Land „Y".

Änderungen des Sicherheitsgrades der im Mobilfunkgerät 2 verwendeten Kryptographiefunktionen 11, 23, respektive von diesen Kryptographiefunktionen 11, 23 verwendeten Sicherheitsparametern, können dem Benutzer, beispielsweise durch programmierte Funktionen des Sicherheitsgradbestimmungsmoduls 12, 24, mittels der Anzeige 21 mitgeteilt werden. Es ist auch möglich, dass sich der Benutzer des Mobilfunkgeräts 2 selber über aktuelle Sicherheitsgrade, respektive momentan verwendete Sicherheitsparameter, informieren kann, indem er beispielsweise entsprechende programmierte Funktionen des Sicherheitsgradbestimmungsmoduls 12, 24 aktiviert, zum Beispiel mittels der Bedienungselemente 22 des Mobilfunkgeräts 2.

Neben den eingangs erwähnten Vorteilen für die Hersteller von Produkten mit kryptographischen Funktionen (11, 23) ergeben sich auch Möglichkeiten, die vorliegende Erfindung wirtschaftlich direkt zu vermarkten. Zum Beispiel können Kommunikationsendgeräte und/oder Chipkarten hergestellt und verkauft werden, die ein erfindungsgemässes Sicherheitsgradbestimmungsmodul umfassen. Es ist auch möglich Computer-lesbare Datenträger herzustellen und zu verkaufen, oder unter Lizenzgebühren abzugeben, welche Datenträger codierte Daten enthalten, die ein Computer-Programm repräsentieren, welches Computer-Programm ermöglicht, einen Prozessor, insbesondere in einem Kommunikationsendgerät, so zu steuern, dass er den Sicherheitsgrad von verwendeten Kryptographiefunktionen (11, 23), respektive von diesen Kryptographiefunktionen (11, 23) verwendete Sicherheitsparameter, gemäss dem beschriebenen Verfahren situationsabhängig setzt. Computerprogrammelemente, die Computerprogrammcodemittel umfassen, um einen Prozessor, insbesondere in einem Kommunikationsendgerät, so zu steuern, dass er den Sicherheitsgrad von verwendeten Kryptographiefunktionen (11, 23), respektive von diesen Kryptographiefunktionen (1, 23) verwendete Sicherheitsparameter, gemäss dem beschriebenen Verfahren situationsabhängig setzt, können gegen Bezahlung von Lizenzgebühren an Dritte abgegeben werden, welche diese

Computerprogrammelemente in verschiedenste Vorrichtungen integrieren können.

Liste der Bezugszeichen

1 Chipkarte (SIM-Karte)

2 Kommunikationsendgerät (Mobilfunkgerät)

3 Telekommunikationsnetz (Mobilfunknetz)

4 Dienstserver

11 Kryptographiefunktionen

12 Sicherheitsgradbestimmungsmodul

21 Anzeige

22 Bedienungselemente

23 Kryptographiefunktionen

24 Sicherheitsgradbestimmungsmodul

Ansprüche

1. Verfahren um den Sicherheitsgrad von in Kommunikationsendgeräten (2) verwendeten Kryptographiefunktionen (11, 23) zu setzen, welche Kommunikationsendgeräte (2) über Telekommunikationsnetze (3) kommunizieren, dadurch gekennzeichnet,

dass in einem genannten Kommunikationsendgerät (2) situationsanzeigende Parameter von einer sicheren Quelle (3, 4) gesichert über das Telekommunikationsnetz (3) entgegengenommen werden, und

dass im genannten Kommunikationsendgerät (2) basierend auf entgegengenommenen situationsanzeigenden Parametern Sicherheitsparameter bestimmt werden, welche Sicherheitsparameter von genannten Kryptographiefunktionen (11, 23) verwendet werden und den genannten Sicherheitsgrad bestimmen.

2. Verfahren gemäss Anspruch 1, dadurch gekennzeichnet, dass mindestens gewisse genannte situationsanzeigende Parameter dienstspezifische Angaben enthalten, die von einem Dienstserver (4), von welchem das genannte Kommunikationsendgerät (2) Dienste bezieht, gesichert über das Telekommunikationsnetz (3) an das genannte Kommunikationsendgerät (2) übertragen werden.

3. Verfahren gemäss einem der Ansprüche 1 oder 2, dadurch gekennzeichnet, dass mindestens gewisse genannte situationsanzeigende Parameter Angaben über den zulässigen Sicherheitsgrad oder zulässige Sicherheitsparameter enthalten, die von einem Dienstserver (4), von welchem das genannte Kommunikationsendgerät (2) Dienste bezieht, gesichert über das Telekommunikationsnetz (3) an das genannte Kommunikationsendgerät (2) übertragen werden.

4. Verfahren gemäss einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass mindestens gewisse genannte Kommunikationsendgeräte (2) Mobilfunkgeräte sind, und dass mindestens gewisse genannte situationsanzei-

gende Parameter einen Ländercode enthalten, der von einem Mobilfunknetz (3), in welchem das genannte Mobilfunkgerät (2) roamt, an das genannte Mobilfunkgerät (2) übertragen wird.

5. Verfahren gemäss einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass ein genannter Sicherheitsparameter die maximal zulässige Länge von kryptographischen Schlüsseln angibt.

6. Verfahren gemäss einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass ein genannter Sicherheitsparameter Angaben über zulässige kryptographische Algorithmen enthält.

7. Kommunikationsendgerät (2), das über ein Telekommunikationsnetz (3) kommuniziert, dadurch gekennzeichnet,

dass das Kommunikationsendgerät (2) ein Sicherheitsgradbestimmungsmodul (12, 24) umfasst, um den Sicherheitsgrad von im Kommunikationsendgerät (2) verwendeten Kryptographiefunktionen (11, 23) situationsabhängig zu setzen, welches Sicherheitsgradbestimmungsmodul (12, 24) situationsanzeigende Parameter von einer sicheren Quelle (3, 4) gesichert über das Telekommunikationsnetz (3) entgegennimmt, und welches Sicherheitsgradbestimmungsmodul (12, 24) basierend auf entgegengenommenen situationsanzeigenden Parametern Sicherheitsparameter bestimmt, welche Sicherheitsparameter von genannten Kryptographiefunktionen (11, 23) verwendet werden und den genannten Sicherheitsgrad bestimmen.

8. Chipkarte (1), die entfernbar mit einem Kommunikationsendgerät (2) verbunden werden kann, welches Kommunikationsendgerät (2) über ein Telekommunikationsnetz (3) kommuniziert, dadurch gekennzeichnet,

dass die Chipkarte (1) ein Sicherheitsgradbestimmungsmodul (12) umfasst, um den Sicherheitsgrad von im Kommunikationsendgerät (2) verwendeten Kryptographiefunktionen (11) situationsabhängig zu setzen, welches Sicherheitsgradbestimmungsmodul (12) situationsanzeigende Parameter von einer sicheren Quelle (3, 4) gesichert über das Telekommunikationsnetz (3)

entgegennimmt, und welches Sicherheitsgradbestimmungsmodul (12) basierend auf entgegengenommenen situationsanzeigenden Parametern Sicherheitsparameter bestimmt, welche Sicherheitsparameter von genannten Kryptographiefunktionen (11) verwendet werden und den genannten Sicherheitsgrad bestimmen.

9. Computer-lesbarer Datenträger, der codierte Daten enthält, die ein Computer-Programm repräsentieren, welches Computer-Programm ermöglicht, einen Prozessor in einem Kommunikationsendgerät (2), welches Kommunikationsendgerät (2) über ein Telekommunikationsnetz (3) kommuniziert, so zu steuern, dass er den Sicherheitsgrad von im Kommunikationsendgerät (2) verwendeten Kryptographiefunktionen (11, 23) situationsabhängig setzt, wobei er situationsanzeigende Parameter von einer sicheren Quelle (3, 4) gesichert über das Telekommunikationsnetz (3) entgegennimmt, und wobei er basierend auf entgegengenommenen situationsanzeigenden Parametern Sicherheitsparameter bestimmt, welche Sicherheitsparameter von genannten Kryptographiefunktionen (11, 23) verwendet werden und den genannten Sicherheitsgrad bestimmen.

10. Computerprogrammelement umfassend: Computerprogrammcodemittel, um einen Prozessor in einem Kommunikationsendgerät (2), welches Kommunikationsendgerät (2) über ein Telekommunikationsnetz (3) kommuniziert, so zu steuern, dass er den Sicherheitsgrad von im Kommunikationsendgerät (2) verwendeten Kryptographiefunktionen (11, 23) situationsabhängig setzt, wobei er situationsanzeigende Parameter von einer sicheren Quelle (3, 4) gesichert über das Telekommunikationsnetz (3) entgegennimmt, und wobei er basierend auf entgegengenommenen situationsanzeigenden Parametern Sicherheitsparameter bestimmt, welche Sicherheitsparameter von genannten Kryptographiefunktionen (11, 23) verwendet werden und den genannten Sicherheitsgrad bestimmen.

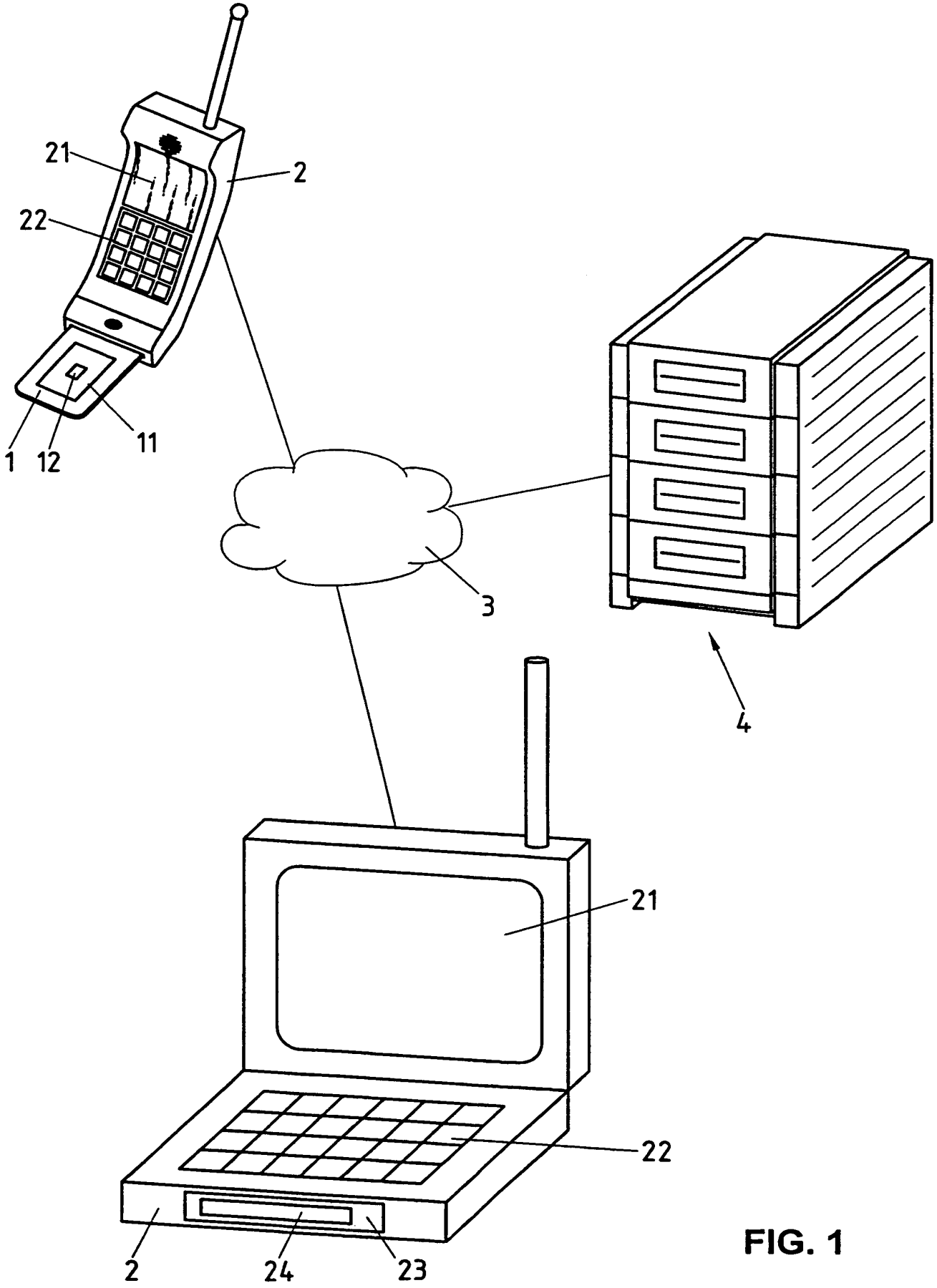


FIG. 1

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT [redacted] DE[redacted]EBIET DES PATENTWE[redacted]NS [redacted]

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts 150973.1/DV/tr	**WEITERES VORGEHEN**	siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5
Internationales Aktenzeichen PCT/CH 99/ 00336	Internationales Anmeldedatum *(Tag/Monat/Jahr)* 21/07/1999	(Frühestes) Prioritätsdatum *(Tag/Monat/Jahr)*
Anmelder SWISSCOM AG et al.		

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 2 Blätter.

[X] Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. **Grundlage des Berichts**

   a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.

   [ ] Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

   b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das

   [ ] in der internationalen Anmeldung in schriftlicher Form enthalten ist.

   [ ] zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

   [ ] Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

   [ ] Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. [ ] **Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen** (siehe Feld I).

3. [ ] **Mangelnde Einheitlichkeit der Erfindung** (siehe Feld II).

4. Hinsichtlich der **Bezeichnung der Erfindung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut von der Behörde wie folgt festgesetzt:

5. Hinsichtlich der **Zusammenfassung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. 1

   [X] wie vom Anmelder vorgeschlagen

   [ ] keine der Abb.

   [ ] weil der Anmelder selbst keine Abbildung vorgeschlagen hat.

   [ ] weil diese Abbildung die Erfindung besser kennzeichnet.

INTERNATIONAL SEARCH REPORT

Inte. ional Application No
PCT/CH 99/00336

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04Q7/38

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 99 09765 A (ERICSSON GE MOBILE INC) 25 February 1999 (1999-02-25) page 8, line 8 -page 9, line 17 page 10, line 8 -page 11, line 17 page 12, line 16 - line 27	1-4,7-10
A	EP 0 779 760 A (NOKIA MOBILE PHONES LTD) 18 June 1997 (1997-06-18) column 4, line 2 - line 33 column 6, line 15 -column 8, line 12	1-3,7-10
A	PATENT ABSTRACTS OF JAPAN vol. 1998, no. 14, 31 December 1998 (1998-12-31) -& JP 10 247936 A (MATSUSHITA ELECTRIC IND CO LTD), 14 September 1998 (1998-09-14) abstract	1,2,7-10

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 March 2000	31/03/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Heinrich, D

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter onal Application No
PCT/CH 99/00336

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9909765 A	25-02-1999	US 5781628 A AU 9292998 A	14-07-1998 08-03-1999
EP 0779760 A	18-06-1997	FI 956036 A	16-06-1997
JP 10247936 A	14-09-1998	NONE	

INTERNATIONALER RECHERCHENBERICHT

Inte. ...onales Aktenzeichen
PCT/CH 99/00336

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04Q7/38

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 H04Q

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der Internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	WO 99 09765 A (ERICSSON GE MOBILE INC) 25. Februar 1999 (1999-02-25) Seite 8, Zeile 8 -Seite 9, Zeile 17 Seite 10, Zeile 8 -Seite 11, Zeile 17 Seite 12, Zeile 16 - Zeile 27	1-4,7-10
A	EP 0 779 760 A (NOKIA MOBILE PHONES LTD) 18. Juni 1997 (1997-06-18) Spalte 4, Zeile 2 - Zeile 33 Spalte 6, Zeile 15 -Spalte 8, Zeile 12	1-3,7-10
A	PATENT ABSTRACTS OF JAPAN vol. 1998, no. 14, 31. Dezember 1998 (1998-12-31) -& JP 10 247936 A (MATSUSHITA ELECTRIC IND CO LTD), 14. September 1998 (1998-09-14) Zusammenfassung	1,2,7-10

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem Internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem Internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem Internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der Internationalen Recherche	Absendedatum des Internationalen Recherchenberichts
20. März 2000	31/03/2000

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Heinrich, D

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Inter. nales Aktenzeichen
PCT/CH 99/00336

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 9909765 A	25-02-1999	US 5781628 A AU 9292998 A	14-07-1998 08-03-1999
EP 0779760 A	18-06-1997	FI 956036 A	16-06-1997
JP 10247936 A	14-09-1998	KEINE	

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

Aktenzeichen des Anmelders oder Anwalts	WEITERES VORGEHEN	siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsberichts (Formblatt PCT/IPEA/416)
150973.1/DV/tr		
Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	Prioritätsdatum *(Tag/Monat/Tag)*
PCT/CH99/00336	21/07/1999	21/07/1999
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK H04Q7/38		
Anmelder SWISSCOM AG et al.		

1. Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationalen vorläufigen Prüfung beauftragten Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.

2. Dieser BERICHT umfaßt insgesamt 6 Blätter einschließlich dieses Deckblatts.

   ☒ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

   Diese Anlagen umfassen insgesamt 6 Blätter.

3. Dieser Bericht enthält Angaben zu folgenden Punkten:

   - I ☒ Grundlage des Berichts
   - II ☐ Priorität
   - III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
   - IV ☐ Mangelnde Einheitlichkeit der Erfindung
   - V ☒ Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
   - VI ☐ Bestimmte angeführte Unterlagen
   - VII ☐ Bestimmte Mängel der internationalen Anmeldung
   - VIII ☐ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags	Datum der Fertigstellung dieses Berichts
29/04/2000	28.02.2001
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde: Europäisches Patentamt D-80298 München Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Bevollmächtigter Bediensteter Banerjea, R Tel. Nr. +49 89 2399 7467

Formblatt PCT/IPEA/409 (Deckblatt) (Januar 1994)

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/CH99/00336

I. Grundlage des Berichts

1. Dieser Bericht wurde erstellt auf der Grundlage (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigefügt, weil sie keine Änderungen enthalten.)*:
Beschreibung, Seiten:

1,3-9	ursprüngliche Fassung			
2,2a	eingegangen am	10/01/2001	mit Schreiben vom	08/01/2001

Patentansprüche, Nr.:

1-8	eingegangen am	10/01/2001	mit Schreiben vom	08/01/2001

Zeichnungen, Blätter:

1/1	ursprüngliche Fassung

2. Hinsichtlich der **Sprache**: Alle vorstehend genannten Bestandteile standen der Behörde in der Sprache, in der die internationale Anmeldung eingereicht worden ist, zur Verfügung oder wurden in dieser eingereicht, sofern unter diesem Punkt nichts anderes angegeben ist.

   Die Bestandteile standen der Behörde in der Sprache: zur Verfügung bzw. wurden in dieser Sprache eingereicht; dabei handelt es sich um

   ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen Recherche eingereicht worden ist (nach Regel 23.1(b)).

   ☐ die Veröffentlichungssprache der internationalen Anmeldung (nach Regel 48.3(b)).

   ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen vorläufigen Prüfung eingereicht worden ist (nach Regel 55.2 und/oder 55.3).

3. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale vorläufige Prüfung auf der Grundlage des Sequenzprotokolls durchgeführt worden, das:

   ☐ in der internationalen Anmeldung in schriftlicher Form enthalten ist.

   ☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

   ☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

   ☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

   ☐ Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

   ☐ Die Erklärung, daß die in computerlesbarer Form erfassten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

4. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

   ☐ Beschreibung, Seiten:

   ☐ Ansprüche, Nr.:

   ☐ Zeichnungen, Blatt:

5. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)).

   (Auf Ersatzblätter, die solche Änderungen enthalten, ist unter Punkt 1 hinzuweisen;sie sind diesem Bericht beizufügen).

6. Etwaige zusätzliche Bemerkungen:

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja:	Ansprüche	1-8
	Nein:	Ansprüche	
Erfinderische Tätigkeit (ET)	Ja:	Ansprüche	1-8
	Nein:	Ansprüche	
Gewerbliche Anwendbarkeit (GA)	Ja:	Ansprüche	1-8
	Nein:	Ansprüche	

2. Unterlagen und Erklärungen
   siehe Beiblatt

A. Bemerkungen zu Abschnitt V

1. Die Erfindung bezieht sich auf ein Verfahren zum situationsabhängigen Setzen des Sicherheitsgrads von Kryptographiefunktionen gemäß den Merkmalen von **Anspruch 1**, sowie auf ein Kommunikationsendgerät bzw. eine Chipkarte welches ein entsprechendes Sicherheitsgradbestimmungsmodul umfaßt gemäß jeweils den Merkmalen der **Ansprüche 5 und 6**, sowie auf einen entsprechenden Computer-lesbaren Datenträger und ein Computerprogrammelement gemäß jeweils den Merkmalen der **Ansprüche 7 und 8**.

2. Um vertrauliche Daten bei der Übertragung über Telekommunikationsnetze vor dem Zugriff durch unberechtigte Drittparteien zu schützen ist es **generell** üblich, Kryptographieverfahren einzusetzen. In der **EP-A-0 779 760** wird z.B. ein Verfahren bzw. eine Vorrichtung zum situationsabhängigen Setzen des Sicherheitsgrads von Kryptographiefunktionen, die in Kommunikationsendgeräten verwendet werden offenbart. Diese Kommunikationsendgeräte kommunizieren über Telekommunikationsnetze. In diesem bereits bekannten Verfahren werden in einem solchen Kommunikationsendgerät situationsanzeigende Parameter von einer sicheren Quelle gesichert über das Telekommunikationsnetz entgegengenommen.

3. Ein wesentlicher **Nachteil** des bekannten Verfahrens bzw. der bekannten Vorrichtung besteht darin, daß die Hersteller von solchen Kryptographieprodukten, den nationalen Vorschriften und gesetzlichen Bestimmungen bezüglich Sicherheitsgrad und Verwendung von gewissen Sicherheitsparameter unterliegen. Somit müssen die Hersteller solcher bekannten Verfahren bzw. Vorrichtungen unterschiedliche Kryptographieprodukte in die verschiedenen Zielmärkte liefern.

4. Der vorliegenden Erfindung liegt somit die **Aufgabe** zugrunde, ausgehend vom oben genannten Stand der Technik, ein effizienteres Verfahren sowie dafür geeignete Vorrichtung vorzuschlagen, welche es ermöglichen, den Sicherheitsgrad von in Kommunikationsendgeräten verwendeten Kryptographiefunktionen situationsabhängig automatisch anzupassen.

5. Zur **Lösung** dieser Aufgabe ist ein Verfahren zum situationsabhängigen Setzen des Sicherheitsgrads von Kryptographiefunktionen gemäß den Merkmalen von **Anspruch 1**, sowie ein Kommunikationsendgerät bzw. eine Chipkarte welches ein entsprechendes Sicherheitsgradbestimmungsmodul umfaßt gemäß jeweils den Merkmalen der **Ansprüche 5 und 6**, sowie eine entsprechender Computer-lesbarer Datenträger und ein Computerprogrammelement gemäß jeweils den Merkmalen der **Ansprüche 7 und 8** vorgesehen.

   Die **Erfindung** besteht im wesentlichen darin, daß im genannten Kommunikationsendgerät basierend auf aktuellen entgegengenommenen situationsanzeigenden Parametern Sicherheitsparameter bestimmt werden, welche Sicherheitsparameter im Kommunikationsendgerät den betreffenden situationsanzeigenden Parametern zugeordnet sind, und welche Sicherheitsparameter **die Länge von kryptographischen Schlüsseln und/oder die Benennung von kryptographischen Algorithmen umfassen**, die von den genannten Kryptographiefunktionen verwendet werden und die **die Höhe** (d.h. den Abstufungswert) des Sicherheitsgrads dieser genannten Kryptographiefunktionen bestimmen.

6. Die Erfindung bietet den **Vorteil**, daß keine unterschiedlichen Kryptographieprodukte in verschiedene Zielmärkte geliefert werden müssen und verschiedene Abstufungen des Sicherheitsgrads für unterschiedliche Dienste und Anwendungen dynamisch und flexibler gesetzt bzw. angepaßt werden können.

7. Der Gegenstand der vorliegenden Erfindung wird auch durch die weiteren, im Internationalen Recherchenbericht genannten Dokumente weder offenbart, noch nahegelegt, da diese Dokumente lediglich einen in bezug auf die vorliegende Erfindung sehr allgemeinen Stand der Technik im Fachgebiet der Kryptographie darstellen.

8. Der Gegenstand der unabhängigen **Ansprüche 1, 5, 6, 7 und 8** wird daher als neu und erfinderisch angesehen, Artikel 33(2) und (3) PCT.

9. Die **Ansprüche 2 bis 4** sind abhängig von Anspruch 1 und erfüllen somit ebenfalls die Erfordernisse des Artikels 33(2) und (3) PCT hinsichtlich Neuheit und erfinderischer Tätigkeit.

10. Die vorliegende Erfindung ist offensichtlich auch gewerblich anwendbar, Artikel 33(4) PCT.

Märkte erweist sich dabei als keine optimale Lösung, da die Produkteversionen und insbesondere auch Kombinationen mit anderen Produkten, in welche die Kryptographieprodukte integriert werden, viel zu zahlreich sind und einen unwirtschaftlichen Mehraufwand mit sich bringen. In alternativen Lösungen wird zwar das gleiche Produkt überallhin ausgeliefert, aber gewisse Teile, die den national auferlegten Restriktionsbestimmungen unterliegen, werden vor der Produktauslieferung durch Schalter deaktiviert, beispielsweise mittels softwaremässigen Schaltern, die durch Setzen von sogenannten Flags ein- respektive ausgeschaltet werden. Das Problem dieser alternativen Lösung besteht darin, dass diese Schalter oft auch durch Drittparteien verändert werden können, beispielsweise durch sogenannte Programmpatches, die die erwähnten Flags manipulieren können.

In der Patentanmeldung EP 779 760 A1 wird ein Verfahren beschrieben, um in einer Mobilstation dem betreffenden Benutzer anzuzeigen, ob die Datenübertragung zwischen der Mobilstation und dem Mobilkommunikationssystem verschlüsselt wird oder nicht. Um dies zu erreichen werden gemäss der Lehre von EP 779 760 A1 die zwischen der Mobilstation und dem Mobilkommunikationssystem ausgetauschten Signale überwacht, und auf der Basis der überwachten Signale dem Benutzer angezeigt, ob die ausgetauschten Daten verschlüsselt sind oder nicht, beispielsweise indem dem Benutzer für den verschlüsselten Modus und den unverschlüsselten Modus verschiedene akustische Signale wiedergegeben werden. In Übereinstimmung mit den GSM-Normen (Global System for Mobile Communication) wird der Verschlüsselungsmodus gemäss EP 779 760 A1 durch Einheiten im Mobilkommunikationssystem mittels sogenannten „cipher mode command" Meldungen in den verschlüsselten Modus, respektive in den unverschlüsselten Modus gesetzt. Gemäss der Lehre von EP 779 760 A1 kann der aktuelle Verschlüsselungsmodus beispielsweise durch den Zentralprozessor der Mobilstation in einem dafür vorgesehenen Anzeigedatenfeld angegeben werden, das beispielsweise ein einziges Informationsbit umfasst.

Es ist eine Aufgabe dieser Erfindung, ein neues und besseres Verfahren sowie dafür geeignete Vorrichtungen vorzuschlagen, welche es ermögli-

chen, den Sicherheitsgrad von in Kommunikationsendgeräten verwendeten Kryptographiefunktionen, insbesondere situationsabhängig, zu setzen.

Gemäss der vorliegenden Erfindung wird dieses Ziel insbesondere durch die Elemente der unabhängigen Ansprüche erreicht. Weitere vorteilhafte Ausführungsformen gehen ausserdem aus den abhängigen Ansprüchen und der Beschreibung hervor.

Dieses Ziel wird durch die vorliegende Erfindung insbesondere dadurch erreicht, dass in einem Kommunikationsendgerät, welches über Telekommunikationsnetze kommuniziert, situationsanzeigende Parameter von einer sicheren Quelle, die beispielsweise mittels einem digitalen Zertifikat als sichere Quelle authentifiziert wird, gesichert über das Telekommunikationsnetz entgegengenommen werden, beispielsweise direkt, ohne Beeinflussungsmöglichkeiten durch andere Elemente, aus einem chiffrierten Datenobjekt mit zertifiziertem Schlüssel oder als nicht beeinflussbarer Bestandteil des im betreffenden Telekommunikationsnetz verwendeten Protokolls, und dass im Kommunikationsendgerät basierend auf entgegengenommenen situationsanzeigenden Parametern Sicherheitsparameter, zum Beispiel die maximal zulässige Länge von kryptographischen Schlüsseln oder zugelassene

Ansprüche

1. Verfahren zum situationsabhängigen Setzen des Sicherheitsgrads von Kryptographiefunktionen (11, 23), die in Kommunikationsendgeräten (2) verwendet werden, welche Kommunikationsendgeräte (2) über Telekommunikationsnetze (3) kommunizieren, in welchem Verfahren in einem genannten Kommunikationsendgerät (2) situationsanzeigende Parameter von einer sicheren Quelle (3, 4) gesichert über das Telekommunikationsnetz (3) entgegengenommen werden, dadurch gekennzeichnet,

dass im genannten Kommunikationsendgerät (2) basierend auf aktuellen entgegengenommenen situationsanzeigenden Parametern Sicherheitsparameter bestimmt werden, welche Sicherheitsparameter im Kommunikationsendgerät (2) den betreffenden situationsanzeigenden Parametern zugeordnet sind, und welche Sicherheitsparameter die Länge von kryptographischen Schlüsseln und/oder die Benennung von kryptographischen Algorithmen umfassen, die von den genannten Kryptographiefunktionen (11, 23) verwendet werden und die die Höhe des Sicherheitsgrads dieser genannten Kryptographiefunktionen (11, 23) bestimmen.

2. Verfahren gemäss Anspruch 1, dadurch gekennzeichnet, dass mindestens gewisse genannte situationsanzeigende Parameter dienstspezifische Angaben enthalten, die von einem Dienstserver (4), von welchem das genannte Kommunikationsendgerät (2) Dienste bezieht, gesichert über das Telekommunikationsnetz (3) an das genannte Kommunikationsendgerät (2) übertragen werden.

3. Verfahren gemäss einem der Ansprüche 1 oder 2, dadurch gekennzeichnet, dass mindestens gewisse genannte situationsanzeigende Parameter Angaben über den zulässigen Sicherheitsgrad oder zulässige Sicherheitsparameter enthalten, die von einem Dienstserver (4), von welchem das genannte Kommunikationsendgerät (2) Dienste bezieht, gesichert über das Telekommunikationsnetz (3) an das genannte Kommunikationsendgerät (2) übertragen werden.

4. Verfahren gemäss einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass mindestens gewisse genannte Kommunikationsendgeräte (2) Mobilfunkgeräte sind, und dass mindestens gewisse genannte situationsanzeigende Parameter einen Ländercode enthalten, der von einem Mobilfunknetz (3), in welchem das genannte Mobilfunkgerät (2) roamt, an das genannte Mobilfunkgerät (2) übertragen wird.

5. Kommunikationsendgerät (2), das über ein Telekommunikationsnetz (3) kommuniziert, welches Kommunikationsendgerät (2) ein Sicherheitsgradbestimmungsmodul (12, 24) umfasst, um den Sicherheitsgrad von Kryptographiefunktionen (11, 23), die im Kommunikationsendgerät (2) verwendet werden, situationsabhängig zu setzen, welches Sicherheitsgradbestimmungsmodul (12, 24) situationsanzeigende Parameter von einer sicheren Quelle (3, 4) gesichert über das Telekommunikationsnetz (3) entgegennimmt, dadurch gekennzeichnet,

dass das Sicherheitsgradbestimmungsmodul (12, 24) Tabellen oder entsprechende Programminstruktionen umfasst, mittels welchen den aktuellen entgegengenommenen situationsanzeigenden Parametern entsprechende Sicherheitsparameter zugeordnet werden, welche Sicherheitsparameter die Länge von kryptographischen Schlüsseln und/oder die Benennung von kryptographischen Algorithmen umfassen, die von den genannten Kryptographiefunktionen (11, 23) verwendet werden und die die Höhe des Sicherheitsgrads dieser genannten Kryptographiefunktionen (11, 23) bestimmen.

6. Chipkarte (1), die entfernbar mit einem Kommunikationsendgerät (2) verbindbar ist, welches Kommunikationsendgerät (2) über ein Telekommunikationsnetz (3) kommuniziert, welche Chipkarte (1) ein Sicherheitsgradbestimmungsmodul (12) umfasst, um den Sicherheitsgrad von im Kommunikationsendgerät (2) verwendeten Kryptographiefunktionen (11) situationsabhängig zu setzen, welches Sicherheitsgradbestimmungsmodul (12) situationsanzeigende Parameter von einer sicheren Quelle (3, 4) gesichert über das Telekommunikationsnetz (3) entgegennimmt, dadurch gekennzeichnet,

dass das Sicherheitsgradbestimmungsmodul (12, 24) Tabellen oder entsprechende Programminstruktionen umfasst, mittels welchen den aktuellen entgegengenommenen situationsanzeigenden Parametern entsprechende Sicherheitsparameter zugeordnet werden, welche Sicherheitsparameter die Länge von kryptographischen Schlüsseln und/oder die Benennung von kryptographischen Algorithmen umfassen, die von den genannten Kryptographiefunktionen (11, 23) verwendet werden und die die Höhe des Sicherheitsgrads dieser genannten Kryptographiefunktionen (11, 23) bestimmen.

7. Computer-lesbarer Datenträger, der codierte Daten enthält, die ein Computer-Programm repräsentieren, welches Computer-Programm ermöglicht, einen Prozessor in einem Kommunikationsendgerät (2), welches Kommunikationsendgerät (2) über ein Telekommunikationsnetz (3) kommuniziert, so zu steuern, dass er den Sicherheitsgrad von im Kommunikationsendgerät (2) verwendeten Kryptographiefunktionen (11, 23) situationsabhängig setzt, wobei er situationsanzeigende Parameter von einer sicheren Quelle (3, 4) gesichert über das Telekommunikationsnetz (3) entgegennimmt, dadurch gekennzeichnet,

dass das Computer-Programm Tabellen oder entsprechende Programminstruktionen umfasst, mittels welchen den aktuellen entgegengenommenen situationsanzeigenden Parametern entsprechende Sicherheitsparameter zugeordnet werden, welche Sicherheitsparameter die Länge von kryptographischen Schlüsseln und/oder die Benennung von kryptographischen Algorithmen umfassen, die von den genannten Kryptographiefunktionen (11, 23) verwendet werden und die die Höhe des Sicherheitsgrads dieser genannten Kryptographiefunktionen (11, 23) bestimmen.

8. Computerprogrammelement umfassend: Computerprogrammcodemittel, um einen Prozessor in einem Kommunikationsendgerät (2), welches Kommunikationsendgerät (2) über ein Telekommunikationsnetz (3) kommuniziert, so zu steuern, dass er den Sicherheitsgrad von im Kommunikationsendgerät (2) verwendeten Kryptographiefunktionen (11, 23) situationsab-

hängig setzt, wobei er situationsanzeigende Parameter von einer sicheren Quelle (3, 4) gesichert über das Telekommunikationsnetz (3) entgegennimmt, dadurch gekennzeichnet,

dass das Computer-Programm Tabellen oder entsprechende Programminstruktionen umfasst, mittels welchen den aktuellen entgegengenommenen situationsanzeigenden Parametern entsprechende Sicherheitsparameter zugeordnet werden, welche Sicherheitsparameter die Länge von kryptographischen Schlüsseln und/oder die Benennung von kryptographischen Algorithmen umfassen, die von den genannten Kryptographiefunktionen (11, 23) verwendet werden und die die Höhe des Sicherheitsgrads dieser genannten Kryptographiefunktionen (11, 23) bestimmen.

Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

10/031571

Applicant's or agent's file reference 150973.1/DV/tr	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/CH99/00336	International filing date (*day/month/year*) 21 July 1999 (21.07.99)	Priority date (*day/month/year*) 21 July 1999 (21.07.1999)
International Patent Classification (IPC) or national classification and IPC H04Q 7/38		
Applicant	SWISSCOM MOBILE AG	

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 6 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 6 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
29 April 2000 (29.04.00)	28 February 2001 (28.02.2001)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/CH99/00336

I. Basis of the report

1. With regard to the **elements** of the international application:*

☐ the international application as originally filed

☒ the description:

pages 1,3-9, as originally filed

pages _____, filed with the demand

pages 2,2a, filed with the letter of 10 January 2001 (10.01.2001)

☒ the claims:

pages _____, as originally filed

pages _____, as amended (together with any statement under Article 19

pages _____, filed with the demand

pages 1-8, filed with the letter of 10 January 2001 (10.01.2001)

☒ the drawings:

pages 1/1, as originally filed

pages _____, filed with the demand

pages _____, filed with the letter of _____

☐ the sequence listing part of the description:

pages _____, as originally filed

pages _____, filed with the demand

pages _____, filed with the letter of _____

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).

☐ the language of publication of the international application (under Rule 48.3(b)).

☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

☐ contained in the international application in written form.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority in written form.

☐ furnished subsequently to this Authority in computer readable form.

☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

☐ the description, pages _____

☐ the claims, Nos. _____

☐ the drawings, sheets/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* *Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).*

** *Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-8	YES
	Claims		NO
Inventive step (IS)	Claims	1-8	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-8	YES
	Claims		NO

2. Citations and explanations

1. The invention relates to a method, as per the features of **Claim 1**, for setting the security level of cryptographic functions, dependent upon the situation, and also to a communications transmitter and a chip card comprising a corresponding module for determining the security level, as per **Claims 5 and 6** respectively, and also to a corresponding computer-readable data carrier and a computer program according to **Claims 7 and 8** respectively.

2. It is **common** practice to use cryptographic methods to protect confidential data being transmitted via a telecommunications network from access by unauthorised third parties. In **EP-A-0 779 760**, for example, a method and a device are disclosed for setting the security level, dependent upon the situation, of cryptographic functions used in communications transmitters. Said communications transmitters communicate via telecommunications networks. In said previously disclosed method, such a communication transmitter receives situation-indicator parameters in a secure manner from a secure source via the telecommunications network.

3. A considerable **drawback** of the known method and the known device is that the manufacturers of such cryptographic products are subject to national regulations and legal requirements relating to the security level and use of certain security parameters. In consequence, the manufacturers of such known methods or devices have to deliver different cryptographic products to the different target markets.

4. The **problem** addressed by the present invention, with the prior art as the point of departure, is that of devising an efficient method as well as an appropriate device, thereby enabling the security level of cryptographic functions used in communications transmitters to be automatically adjusted, dependent upon the situation.

5. To **solve** said problem, a method for situation-dependent setting of the security level of cryptographic functions, as per the features of **Claim 1,** as well as a communications transmitter and a chip card comprising a corresponding module for determining the security level, as per **Claims 5 and 6** respectively, as well as a corresponding computer-readable data carrier and a computer program element as per **Claims 7 and 8** respectively, are provided.

The essence of the **invention** is that security parameters are determined in the cited communications transmitter, on the basis of current received situation-indicator parameters, and are assigned in the communications transmitter to the relevant situation-indicator parameters; said

/...

security parameters include **the length of cryptographic keys and/or the nomenclature of cryptographic algorithms**, which are used by the cited cryptographic functions and determine **the height** (i.e. the graduation value) of the security level of said cryptographic functions.

6. The invention offers the **advantage** of eliminating the need to deliver different cryptographic products to different target markets whilst different graduations of the security level, for different purposes, can be more dynamically and flexibly set and adjusted.

7. The subject matter of the present invention is neither disclosed nor suggested in the other prior art cited in the international search report since, in respect of the present invention, said documents constitute no more than very general prior art in the field of cryptography.

8. The subject matter of the independent **Claims 1, 5, 6, 7 and 8** is therefore considered to be novel and to involve an inventive step (PCT Article 33(2) and (3)).

9. **Claims 2 to 4** are dependent on Claim 1 and thus likewise meet the requirements of PCT Article 33(2) and (3) in respect of novelty and inventive step.

10. The present invention is plainly also industrially applicable (PCT Article 33(4)).

deactivated by switches before product delivery, for instance by means of software switches switched on or off by setting so-called flags. The problem with this alternative solution is that these switches can often be changed also by third parties, for example through so-called program patches that are able to manipulate the mentioned flags.

It is an object of this invention to propose a new and better method as well as devices suitable therefor which make it possible to set the degree of security of cryptography functions used in communication terminals, in particular in a situation-dependent way.

This object is achieved according to the present invention through the elements of the independent claims. Further advantageous embodiments follow moreover from the dependent claims and from the specification.

This object is achieved through the present invention in particular in that situation-indicating parameters from a secure source, which is authenticated as a secure source by means of a digital certificate, for example, are received over the telecommunication network in a secure way, e.g. directly, without possibilities of being influenced by other elements, in a communication terminal that communicates over telecommunication networks from an encoded data object with certified key or as a component, which cannot be influenced, of the protocol used in the respective telecommunication network, and in that security parameters, for instance the maximal permissible length of cryptographic keys or permitted cryptographic algorithms, are determined in the communication terminal based on received situation-indicating parameters. These security parameters are then used by cryptography functions and determine the degree of security. The advantage of this method is that the degree of security of cryptography functions used in the communication terminal, or respectively of the security parameters applied by these cryptography functions, can be set situation-dependently and dynamically so that differing cryptography products do not have to be supplied in different destination markets and no switches have to be set by manufacturers in a fixed way, the effect of which switches can be cancelled by one-time overwriting.

In an embodiment variant, at least certain situation-dependent parameters contain service-specific data, for example data relating to the type of respective service, which are transmitted in a secure way, e.g. encrypted

Claims

1. A method for setting the degree of security of cryptography functions (11, 23) used in communication terminals (2), which communication terminals (2) communicate via telecommunication networks (3), wherein

situation-indicating parameters are received in a said communication terminal (2) over the telecommunication network (3) from a secure source (3, 4), and

based on received situation-indicating parameters, security parameters are determined in the said communication terminal (2), which security parameters are used by said cryptography functions (11, 23) and determine the said degree of security.

2. The method according to claim 1, wherein at least certain said situation-indicating parameters contain service-specific data which are transmitted in a secure way over the telecommunication network (3) to the said communication terminal (2) by a service server (4) from which the said communication terminal (2) obtains services.

3. The method according to one of the claims 1 or 2, wherein at least certain said situation-indicating parameters contain data about the permissible degree of security or permissible security parameters which are transmitted in a secure way over the telecommunication network (3) to the said communication terminal (2) by a service server (4) from which the said communication terminal (2) obtains services.

4. The method according to one of the claims 1 to 3, wherein at least certain said communication terminals (2) are mobile radio devices, and at least certain said situation-indicating parameters contain a country code which is transmitted to the said mobile radio device (2) by a mobile radio network (3) in which the said mobile radio device (2) is roaming.

5. The method according to one of the claims 1 to 4, wherein a said security parameter indicates the maximal permissible length of cryptographic keys.

6. The method according to one of the claims 1 to 5, wherein a said security parameter contains data about permissible cryptographic algorithms.

7. A communication terminal (2) which communicates via a telecommunication network (3), wherein

the communication terminal (2) includes a degree-of-security-determining module (12, 24) in order to set in a situation-dependent way the degree of security of cryptography functions (11, 23) used in the communication terminal (2), which degree-of-security-determining module (12, 24) receives situation-indicating parameters from a secure source (3, 4) in a secure way over the telecommunication network (3), and which degree-of-security-determining module (12, 24) determines security parameters based on received situation-indicating parameters, which security parameters are used by said cryptography functions (11, 23) and determine the said degree of security.

8. A chipcard (1) which is able to be removably connected to the communication terminal (2), which communication terminal (2) communicates via a telecommunication network (3), wherein

the chipcard (1) includes a degree-of-security-determining module (12) in order to set in a situation-dependent way the degree of security of cryptography functions (11) used in the communication terminal (2), which degree-of-security-determining module (12) receives situation-indicating parameters in a secure way over the telecommunication network (3) from a secure source (3, 4) and which degree-of-security-determining module (12) determines security parameters based on received situation-indicating parameters, which security parameters are used by said cryptography functions (11) and determine the said degree of security.

9. A computer-readable data carrier containing coded data representing a computer program, which computer program makes it possible to control a processor in a communication terminal (2), which communication terminal (2) communicates via a telecommunication network (3), such that it sets in a situation-dependent way the degree of security of cryptography functions (11, 23) used in the communication terminal (2), whereby it receives situation-indicating parameters over the telecommunication network (3) from a secure source (3, 4) in a secure way, and whereby it determines security parameters based on the received situation-indicating parameters, which security parameters are used by said cryptography functions (11, 23) and determine the said degree of security.

10. A computer program element having: computer program code means in order to control a processor in a communication terminal (2), which communication terminal (2) communicates via a telecommunication network (2), such that the processor sets in a situation-dependent way the degree of security of cryptography functions (11, 23) used in the communication terminal (2), whereby it receives situation-indicating parameters from a secure source (3, 4) over the telecommunication network (3) in a secure way and whereby it determines security parameters based on received situation-indicating parameters, which security parameters are used by said cryptography functions (11, 23) and determine the said degree of security.

THE FOLLOWING IS THE ENGLISH TRANSLATION OF THE ANNEXES TO THE INTERNATIONAL PRELIMINARY EXAMINATION REPORT : AMENDED SHEETS (Pages 2, 2a, 8, 9, and 10).

deactivated by switches before product delivery, for instance by means of software switches switched on or off by setting so-called flags. The problem with this alternative solution is that these switches can often be changed also by third parties, for example through so-called program patches that are able to manipulate the mentioned flags.

Described in the patent application EP 779 760 A1 is a method to indicate to a respective user in a mobile station whether the data transmission between the mobile station and the mobile communications system is encrypted or not. To achieve this, according to the teachings of EP 779 760 A1, the signals exchanged between the mobile station and the mobile communications system are monitored, and on the basis of the monitored signals it is indicated to the user whether the exchanged data are encrypted or not, for example by reproducing different acoustical signals for the user for the encrypted mode and for the unencrypted mode. In accordance with GSM standards (Global System for Mobile Communication), the encryption mode according to EP 779 760 A1 is set in the encrypted mode, or respectively in the unencrypted mode, by units in the mobile communications system by means of so-called "cipher code command" messages. According to the teaching of EP 779 760 A1, the current encryption mode can be indicated by the central processor of the mobile station, for example, in a display data field provided therefor which comprises e.g. a single information bit.

It is an object of this invention to propose a new and better method as well as devices suitable therefor which make it possible to set the degree of security of cryptography functions used in communication terminals, in particular in a situation-dependent way.

This object is achieved according to the present invention through the elements of the independent claims. Further advantageous embodiments follow moreover from the dependent claims and from the specification.

This object is achieved through the present invention in particular in that situation-indicating parameters from a secure source, which is authenticated as a secure source by means of a digital certificate, for example, are received via the telecommunication network in a secure way, e.g. directly, without

possibilities of being influenced by other elements, in a communication terminal that communicates over telecommunication networks from an encoded data object with certified key or as a component, which cannot be influenced, of the protocol used in the respective telecommunication network, and in that security parameters, for instance the maximal permissible length of cryptographic keys or permitted cryptographic algorithms, are determined in the communication terminal based on received situation-indicating parameters. These security parameters are then used by cryptography functions and determine the degree of security. The advantage of this method is that the degree of security of cryptography functions used in the communication terminal, or respectively of the security parameters applied by these cryptography functions, can be set situation-dependently and dynamically so that differing cryptography products do not have to be supplied in different destination markets and no switches have to be set by manufacturers in a fixed way, the effect of which switches can be cancelled by one-time overwriting.

In an embodiment variant, at least certain situation-dependent parameters contain service-specific data, for example data relating to the type of respective service, which are transmitted in a secure way, e.g. encrypted

Claims

1. A method for setting in a situation-dependent way the degree of security of cryptography functions (11, 23) which are used in communication terminals (2), which communication terminals (2) communicate via telecommunication networks (3), in which method situation-indicating parameters are received in a said communication terminal (2) over the telecommunication network (3) from a secure source (3, 4), wherein

based on current received situation-indicating parameters, security parameters are determined in the said communication terminal (2), which security parameters are associated in the communications terminal (2) with the respective situation-indicating parameters, and which security parameters include the length of cryptographic keys and/or the designation of cryptographic algorithms which are used by the said cryptography functions (11, 23) and which determine the height of the degree of security of these said cryptography functions (11, 23).

2. The method according to claim 1, wherein at least certain said situation-indicating parameters contain service-specific data which are transmitted in a secure way over the telecommunication network (3) to the said communication terminal (2) by a service server (4) from which the said communication terminal (2) obtains services.

3. The method according to one of the claims 1 or 2, wherein at least certain said situation-indicating parameters contain data about the permissible degree of security or permissible security parameters which are transmitted in a secure way over the telecommunication network (3) to the said communication terminal (2) by a service server (4) from which the said communication terminal (2) obtains services.

4. The method according to one of the claims 1 to 3, wherein at least certain said communication terminals (2) are mobile radio devices, and at least certain said situation-indicating parameters contain a country code which is transmitted to the said mobile radio device (2) by a mobile radio network (3) in which the said mobile radio device (2) is roaming.

5. A communication terminal (2) which communicates via a telecommuni-

cation network (3), which communication terminal (2) includes a degree-of-security-determining module (12, 24) in order to set in a situation-dependent way the degree of security of cryptography functions (11, 23) which are used in the communication terminal (2), which degree-of-security-determining module (12, 24) receives situation-indicating parameters from a secure source (3, 4) in a secure way over the telecommunication network (3), wherein

the degree-of-security-determining module (12, 24) includes tables or corresponding program instructions by means of which corresponding security parameters are associated with the current received situation-indicating parameters, which security parameters include the length of cryptographic keys and/or the designation of cryptographic algorithms which are used by the said cryptography functions (11, 23) and which determine the height of the degree of security of these said cryptography functions (11, 23).

6. A chipcard (1) which is removably connectible to the communication terminal (2), which communication terminal (2) communicates via a telecommunication network (3), which chipcard (1) includes a degree-of-security-determining module (12) in order to set in a situation-dependent way the degree of security of cryptography functions (11) used in the communication terminal (2), which degree-of-security-determining module (12) receives situation-indicating parameters in a secure way over the telecommunication network (3) from a secure source (3, 4), wherein

the degree-of-security-determining module (12) includes tables or corresponding program instructions by means of which corresponding security parameters are associated with the current received situation-indicating parameters, which security parameters include the length of cryptographic keys and/or the designation of cryptographic algorithms which are used by the said cryptography functions (11, 23) and which determine the height of the degree of security of these said cryptography functions (11, 23).

7. A computer-readable data carrier containing coded data representing a computer program, which computer program makes it possible to control a processor in a communication terminal (2), which communication terminal (2) communicates over a telecommunication network (3), such that it sets in a situation-dependent way the degree of security of cryptography functions (11,

AMENDED PAGE

23) used in the communication terminal (2), whereby it receives situation-indicating parameters over the telecommunication network (3) from a secure source (3, 4) in a secure way, wherein

the computer program includes tables or corresponding instructions by means of which corresponding security parameters are associated with the current received situation-indicating parameters, which security parameters include the length of cryptographic keys and/or the designation of cryptographic algorithms which are used by the said cryptography functions (11, 23) and which determine the height of the degree of security of these said cryptography functions (11, 23).

8. A computer program element having: computer program code means in order to control a processor in a communication terminal (2), which communication terminal (2) communicates via a telecommunication network (3), such that the processor sets in a situation-dependent way the degree of security of cryptography functions (11, 23) used in the communication terminal (2), whereby it receives situation-indicating parameters over the telecommunication network (3) from a secure source (3, 4) in a secure way, wherein

the computer program includes tables or corresponding program instructions by means of which corresponding security parameters are associated with the current received situation-indicating parameters, which security parameters include the length of cryptographic keys and/or the designation of cryptographic algorithms, which are used by the said cryptography functions (11, 23) and which determine the height of the degree of security of these said cryptography functions (11, 23).